⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－124155

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和63年(1988)5月27日
G 06 F 12/14	320	D－7737－5B	

審査請求　未請求　発明の数 1　（全7頁）

㊹発明の名称　記憶情報保護装置

㉑特　願　昭62－232748

㉒出　願　昭62(1987)9月18日

優先権主張　㉜1986年11月5日㉝米国(US)㉛927298

㉒発明者　ステイーヴ・ハリス・ヴアインアート　アメリカ合衆国ニューヨーク州ピークスキル、フオツクス・ヒル・ロード11番地

㉑出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション　アメリカ合衆国10504、ニューヨーク州　アーモンク（番地なし）

㉔代理人　弁理士　山本　仁朗　外1名

明　細　書

1．発明の名称　記憶情報保護装置

2．特許請求の範囲

(a) 情報を記憶した電子回路の付近に電磁エネルギを分布させるための手段と、

(b) 上記エネルギを感知する手段と、

(c) クロック回路と、

(d) 上記感知手段の出力をサンプルし記憶するように上記クロック回路によって周期的にクロック制御されるサンプル・ホールド回路と、

(e) 上記感知手段の出力を上記サンプル・ホールド回路の出力に依存した基準レベルと比較し、上記エネルギの変動を検出した時上記電子回路への侵入を示す信号を発生する手段と、

(f) 上記信号に応答して上記電子回路又はその中の記憶情報を破壊するための手段と、

を有する記憶情報保護装置。

3．発明の詳細な説明

A．産業上の利用分野

本発明は電子的に記憶される情報のための物理的安全保護技術に関する。

B．従来技術

機械読取り可能な形で入れられているプログラム又はデータを保護するためにコンピュータ業界で取られている伝統的な方法は、コンピュータ設置環境の物理的保護又はこのような保護と何らかの法的保護との組合せを用いるものである。また、許可されない者が不正入手情報を使用できないようにするために暗号化方法も用いられている。パーソナル・コンピュータの領域では、多くの様々なソフトウェア・コピー保護方式が用いられているが、すべてのものはプログラムに組込んだある種のソフトウェア・トラップに基くものであり、徹底した侵害者に対しては有効でない。

米国特許第4471163号はソフトウェア保護機構を例示している。記憶情報の安全保護を図るために、この特許は、プログラム・ロックを装

着する回路板を上下の保護プレートで包囲することを示している。構成要素のための電池電力は保護プレートの内面に取付けた導体を通して供給される。この技術によれば、プリント回路板上の構成要素にアクセスしようとする者は必ず少なくとも一方の保護プレートを動かさねばならず、結果として、電力供給リードを破壊することになる。保護すべき情報を記憶したメモリが電力を必要とするときは、この電力線リードの破壊は、侵入者が求めている情報を破壊し、従って情報が保護されることになる。

米国特許第４４７１１６３号の保護機構は、電力線リードが直接取付けられている保護プレート部分を動かした時にしか有効に働かない。このようなプログラム・ロックに何度かアクセスしたことがある徹底した侵害者であれば、保護の程度を知るために何個かの回路板を破壊するとしても、このような保護の裏をかくことは容易にできることである。

情報入手のために装置又は機械設置場所に対してなされる侵入行為がいくつかの段階で行なわれることは想像できることである。

(1) 包囲体又は包囲体及びカバーの取外し
(2) 安全保護センサの位置及び機能の識別
(3) センサを回避して次の保護レベルへ侵入する、

などである。

このような注意深く手順を踏んだ方法を使うと、十分な時間と資源さえあれば、現存する保護システムを打破することが可能である。

一方、侵入検出装置あるいは警報装置の大部分は所望の質の検出／警報システムを実現するために２つの相反する要件の妥協を取っている。即ち、１つは装置の感度が極力高いことであり、もう１つは装置が環境の変化（例えば温度、圧力、湿度などの変化）の影響を受けると共に老化（これは電源や、抵抗、キャパシタなどの装置パラメータを変動させる）を生じ、誤検出あるいは誤警報を生じやすくなることである。そのため、装置パラメータが変化しても誤動作が生じないように検出感度を制限するのが一般的である。

C．発明が解決しようとする問題点

本発明の目的は、侵入検出の感度を鋭性にすることなく誤検出の問題を軽減できるようにした、電子回路などに記憶される情報を保護する装置を提供することである。

D．問題点を解決するための手段（第１図、第３図）

本発明は電子回路に記憶された情報を保護するものであり、情報を記憶した電子回路の付近に（好ましくはこれを取巻くように）電磁エネルギを分布させるための手段を有する。例えば、これは電子回路を取囲むようにコイル３０を巻回し、電流を流すことによって実現できる。また、電磁エネルギを感知する手段、クロック回路及びサンプル・ホールド回路を有する。サンプル・ホールド回路はクロック回路によって周期的にクロック制御され、感知手段の出力をサンプルし記憶する。例えば、感知手段は、クロック回路によって周期的にリセットされる積分回路によって実現できる。また、比較手段及び比較手段に応答して電子回路又はその中の記憶情報を破壊するための手段が設けられる。比較手段は感知手段の出力とサンプル・ホールド回路の出力に依存した基準レベルとの比較を行ない、電子回路領域への侵入によって電磁エネルギが変動したことを検出した時、侵入を示す信号を発生し、電子回路又は記憶情報の破壊を指示する。

E．実施例

第１図は、チップ１１～１３の形の電子回路を装着した電子回路カード１０を含む、本発明の実施例の保護構造を示している。チップ１１～１３を相互接続するプリント回路配線及びこれらのチップをオフ・カード・コネクタ１４へ接続するプリント回路配線は省略されている。カード１０は保護されるべき情報を記憶するのに用いられる種々の装置の代表として例示している。記憶情報はコネクタ１４を介してアクセス可能であるが、この経路を使った不正アクセスから保護することは本発明の範囲外のことである。本発明の意図は、それ以外の方法で記憶情報にアクセスできないよ

うにすることである。本発明の基本目的は、カードＬＯを含む被保護領域に何も侵入できないようにすることによって達成される。破線５０はカードＬＯを取囲む包囲体を表わしている。

侵入を検出するため、本発明は包囲体内に感知装置を設ける。感知装置は、電磁エネルギを分布させるための手段と、この電磁エネルギ分布を検出するための手段を含む。電磁エネルギ分布の変動又は中断を用いて侵入を感知する。多くのアプリケーションでは、保護されるべき情報は、電力の印加によって情報を維持する揮発性装置に記憶される。本発明は、この実施例では、侵入の検出時に揮発性メモリへの電力の印加を中断（好ましくは電源端子を接地）するか電子装置を破壊するように制御することを意図している。この中断は簡単なスイッチで実施できる。しかし本発明は揮発性の情報記憶装置に特定されない。例えば、ＥＥＰＲＯＭ装置は紫外光の印加によって消去可能であり、紫外光源を設けて、侵入の検出時にこの光源を付勢することも本発明に含まれる。

第１図に示すように、侵入の存在を感知するための１つの素子は、絶縁された導体３０のコイルである。図では、コイルの内部に設けられたカードＬＯが見えるようにするために、隣接する巻回間の間隔を誇張して示しているが、実際には、導体３０のコイルは密な間隔でしっかりと巻回され、小さなプローブ又は他の器具などを挿入できないように、コイルの存在そのものがカードＬＯへのアクセスを物理的に防止するようになっている。従ってアクセスするためには、侵入者は、導体３０のコイルの１つ以上の巻回を動かさねばならない。本発明の意図は、導体を動かすことを禁止あるいは防止するか又は少なくとも、導体を動かそうとする企図を感知することである。良好な実施例では導体３０は約８９μの比較的細い絶縁ニクロム線で形成される。これは２つの利点を与える。１つは、この導体３０は比較的脆弱であり、従って導体を動かそうとすると、又は何かを細工しようとすると、容易に断線が生じることである（このことは、後述するように、検出の基本になる）。

また、侵入者は導体３０の一部を物理的に取外し、取外した導体部分の作用を模擬又は迂回することによって、保護装置に、導体３０が完全に存在するかのように見せかけようとするかも知れないが、ニクロム線は取付けが難しいから、細いニクロム線はこのような細工を一層困難にする。これが２つ目の利点である。勿論、アルミニウム線又はスチール合金線なども使用可能である。

第２図は、プロセッサ・カードＬＯのようなカードが本発明によってどのように保護されるかを示している。包囲体の中には、保護カード２１０が装着されている。保護カード２１０は第３図に示されている回路を含む。プロセッサ・カードＬＯ及び保護カード２１０を取囲むように導体巻線３０が形成される。カードＬＯ、２１０の端部の巻線を支持するために、２つの傾斜部材３５が用いられる。巻線及びその中の構成要素はポッティング材５０で包囲される。巻線３０は１つ以上の巻回を乱さなければプロセッサ・カードＬＯの領域へ侵入できないように配置される。本発明はこのような乱れを検出する。

第３図は検出回路を示している。導体３０の一端は、電源に結合され、他端は積分回路１１０への入力になっている。積分回路１１０の出力は線１１２を介してサンプル・ホールド回路１２０の入力に接続されると共に、線１１３を介して比較回路１３０の入力に接続されている。積分回路１１０はクロック回路１００から線１０１を介して供給される信号により周期的にクロック制御される。サンプル・ホールド回路１２０は、クロック回路１００から導体１０２を介して供給されるもう１つの信号により周期的にリセットされる。サンプル・ホールド回路１２０がリセットされる度に回路１２０は、積分回路１１０の出力の新しいサンプルを取り込む。サンプル・ホールド回路１２０の出力を分圧回路Ｖの端子Ｓに結合される。分圧回路Ｖは正電圧と大地のような２つの基準電位の間に結合される。正電圧と接続点Ｓの間の点Ｈは比較回路１３０の高基準電圧入力に接続され、大地と点Ｓの間の点Ｌは比較回路１３０の低基準

電圧入力に接続される。比較器１３０はクロック１００から線１０３を介して供給される信号によってクロック制御される。これらの回路は市販の普通のものであり、詳しい説明は省略する。

通常の状態では、導体３０に電流が流れ、電流の振巾は導体３０の抵抗に一部依存し、この電流は積分器１１０の入力に流れる。積分器１１０は、時間と共に変動する電圧出力を線１１３に発生する。第４図は導線３０の抵抗及び電源電圧が一定とした時の積分器出力波形を示している。この時積分器１１０の電圧出力は、傾斜波形となる。積分器１１０はクロック１００により時間ｔ１に周期的にリセットされる。リセットされると出力電圧はゼロになり、再び上昇する。

サンプル・ホールド回路１２０へのクロック入力は積分器１１０のリセット時間（ｔ１）の前に、好ましくはその直前に能動状態になり、線１１２の電圧サンプルを取り込む。このサンプルに対応する電圧は点Ｓに与えられ、この電圧は、線１２０の次のクロック・パルスによって新しいサンプルが取り込まれるまで一定に保たれる。

比較器１３０はその入力電圧を、高レベル入力Ｈ及び低レベル入力Ｌの電圧と比較し、高レベルを電圧Ｈよりも大きいか又は低レベル電圧Ｌよりも小さい時回路電力制御回路１４０へ出力を発生する。従って比較器１３０が応答しない窓領域が高レベルＨと低レベルＬの間に存在する。この窓は部分的にはサンプル・ホールド回路１２０によって決まるから、窓は感知装置のパラメータの変化に順応する。制御回路１４０は情報を記憶するチップ１１～１３への電力印加を中断する簡単なスイッチでもよく、あるいはチップ１１～１３の情報記憶維持機能を失わせるように何らかの装置を付勢又は起動するように働く回路でもよい。

ある瞬時に測定した導体の抵抗又はこれを表わす信号を単純に基準値と比較することも可能であるが、この場合は個別の時点で感知するだけとなり、感知時間外に生じる事象をカバーすることができない。従って、クロック周期のほぼ全体にわたる抵抗の測定を積分することによって、抵抗の変化を感知するのが好ましい。積分器の使用はノイズ耐性を高める利点も有する。

明らかなように、比較器１３０への高レベル及び低レベルの基準電圧はサンプル・ホールド回路１２０によって発生される点Ｓの電圧の関数である。この電圧が上昇すると、基準電圧Ｈ、しも上昇し、この電圧が減少すると、Ｈ、しも減少する。しかし比較器１３０は常に、前のサイクルで得たサンプルによって決まる基準レベルと積分器出力を比較する。名目上、パラメータは、比較器１３０がクロック１００によってクロック制御される時に積分器出力が点Ｓの電圧とほぼ等しくなるように構成される。しかし、パラメータの変化のために、比較時刻における積分器１１０の出力がサイクル間で変動すれば、比較器１３０はその変動の程度に依存して出力を発生したり又は発生しなかったりする。積分器出力が基準レベルＨとしの間にあれば、比較器１３０は出力を発生しない。従ってこの回路構成は、導体３０の抵抗変化を感知するための手段として働く。サンプル・ホールド回路１２０及びその分圧器への接続Ｓにより、この回路は適応性を有し、パラメータが変わると基準レベルも変わる。比較器１３０は、１サイクル内の変動が分圧器Ｒ１、Ｒ２、Ｒ３、Ｒ４による変動を超えなければトリップしない。

より具体的にいうと、窓の高い方へスレショルドをE_H、低い方のスレショルドをE_Lとした時、E_HはＩ２＋（Ｖ－Ｉ１）Ｒ２／Ｒ１＋Ｒ２で与えられ、E_LはＩ２－（Ｉ１）Ｒ３／Ｒ３＋Ｒ４で与えられる。ここで、Ｉ２は比較器へのクロック・パルスの時間における積分器出力であり、Ｉ１はサンプル・ホールド回路への前のクロック・パルスの時間における積分器出力であり、Ｒ１、Ｒ２、Ｒ３、Ｒ４はＩ１をＲ２とＲ３の間の入力とする分圧器抵抗である。比較器１３０は、次の条件の時に、不正操作又は侵入を示す出力を発生する。

$I2 > E_H$ 又は

$I2 < E_L$

一定の基準レベルを用いた場合は、装置パラメ

ータの変動によって誤検出が生じる可能性があり、これを防止するためには、特性の変動を見越してスレショルドをゆるく設定しなければならず、検出感度を犠牲する必要があった。しかし本発明のようにサンプル・ホールド回路の出力によって可変の基準レベルを即ち適応性のある基準レベルを設定することにより、比較的小さなトレランスで高い検出感度を維持することができる。スレショルドは1クロック・サイクルで予測される変動に対応できれば十分である。特性の変動速度は通常、クロック速度よりもはるかに遅く、基準レベルはその変動を反映するようにクロック速度で更新されるから、誤検出の可能性が最小になる。

導体30の抵抗は、次の3つの物理的メカニズムのうちのどれかによって変動する：導体30が開放回路になった場合、隣接する巻回線が短絡した場合、及び導体の断面が小さくなるような損傷を受けた場合。侵入はこのような状況の検出によって暗示される。抵抗変化を感知するためには、単位長さ当りの抵抗がある程度大きなコイル線を用いるのが好ましい。

導体30の開放回路は積分器110の出力を急激に変化させ、この急激な変化はほとんど瞬時的であって、間違いなく比較器130によって検出される。

隣接する又は近接した巻回間の短絡をどの程度検出できるかは、短絡回路の形成によって生じる抵抗変化に依存する。もしコイルが1つの線（ストランド）であれば、短絡回路による抵抗変化は検出不能になりうる程度である（1%又はそれ以下）。第5図は短絡回路の効果を増大させる方法を示している。導体30に1つの線を用いる代わりに複数の線を用いる。第5図は4つの線30－1～30－4を示している。線1は電源Vに接続され、線2、3は一緒に結ばれ、線4は積分器入力に接続される。これらの4本の線は次にカードを取囲むように同時に巻回される。巻線の両端は巻線表面の下側に押し込まれる。第5図で短絡回路はSCで示されている。好ましくはないが、別々の線を巻回した後に、線の端を接続して1つの連続導体を形成することも可能である。このような巻線構成によれば、1つの連続した巻線回路上の離れた部分が隣接した巻回を形成するから、隣接する巻回の短絡で大きな抵抗変化を与えることができる。従って、隣接する2つの巻回が短絡しただけで25%もの抵抗変化を得ることができる（4線コイルの場合）。3本以上の線が短絡すると、更に大きな傾向が得られる。

第6図は別の巻線構成を示している。この例では、すべての線を例えば左から右へ巻回し、そしてすべての線の端が例えば左側で得られるように"隠れた"戻り線を用いている。線30－1は左から右へ巻回される第1の部分30－1aと、左端へ戻る連続した部分30－1bを含む。戻り線の部分30－1bは巻線の内部を通して戻される。同様に線30－2は"隠れた"戻り線部分30－2bを有する。すべての線を巻回した時、30－1bの端末部分を30－2aの端に接続し、30－2bの端末部分を30－3aの端に接続することができる。この巻線構成は特に巻線端近くの短絡回路の効果を高める。

本発明による保護を更に高めるために、導体30を巻回した後に、パッケージ全体即ちカード、コイル及び感知回路全体を不透明な無機充填添加架橋エポキシ樹脂ポッティング材で埋込む。アルミナ又はシリカのような充填材を入れると機械加工（侵入者が用いるかも知れない作業）を困難にする利点がある。エポキシに対する別の可能性のある攻撃は溶剤又は化学処理の使用であるが、この場合は導体30の絶縁被覆（例えばポリウレタン又はポリオレフィン）及び恐らくは、導体自体がエポキシよりも先に溶解する。UVレーザ・アブレーションを用いた場合は、これに応答して無機充填材が多量の熱を発生し、この熱は熱勾配による機械的応力によってひび割れを生し、また導線に損傷を与える。導体の破壊は開放回路を生じ、検出されることになる。ポッティング材の中にバイメタルのような、熱によって機械的変形を生じる感熱素子を組込んでおけば、ひび割れなどを助長し、導体損傷の発生確率を高めることができる。

本発明に従ってコイル導体を巻回するやり方には選択の巾がある。普通に各巻回が平行になるように規則的に密に巻回することもでき、あるいは不規則的に巻回することもできる。

導体３０を複数の軸で巻回することにより、即ち、１層目をある軸で巻回し、２層目を別の軸例えば一層目と直角な軸で巻回することにより、カード１０を完全に包囲し、"穴"がない状態にすることができる。

複数本のコイル線を用い複数層に重ね巻きすることは、相殺によりＥＭＩの影響を低減するのに役立ち、また巻線の包囲はＥＭ放射シールドを形成する。また、上述したような感知装置を複数個組込むことができる。

Ｆ．発明の効果

本発明によれば、情報を記憶した電子回路領域への侵入を検出し、検出時に記憶情報を破壊するから、電子回路への物理的なアクセスを用いた記憶情報の不正入手を防止することができ、また比較回路はサンプル・ホールド回路の出力に基づいて定まる可変基準レベルを用いるから、装置パラメータの変動に適応性があり、正確性を保つことができる。

４．図面の簡単な説明

第１図は、本発明の実施例を示す図である。

第２図は、本発明による回路カード保護構造を示す断面図である。

第３図は、感知回路図である。

第４図は、第３図の積分器の出力波形図である。

第５図は、巻線構成を示す図である。

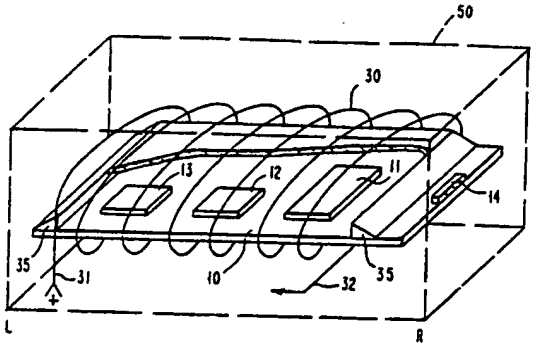
第６図は、代替巻線構成を示す図である。

出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション

代理人　弁理士　山　本　仁　朗

（外１名）

FIG. 1



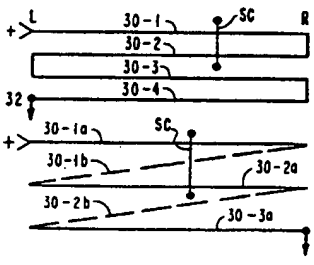


FIG. 5

FIG. 6

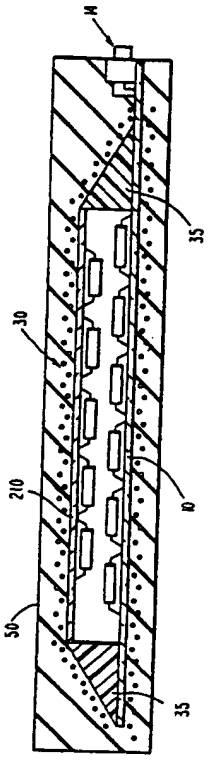


FIG. 2

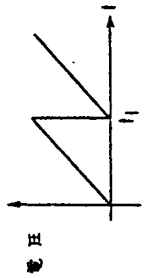
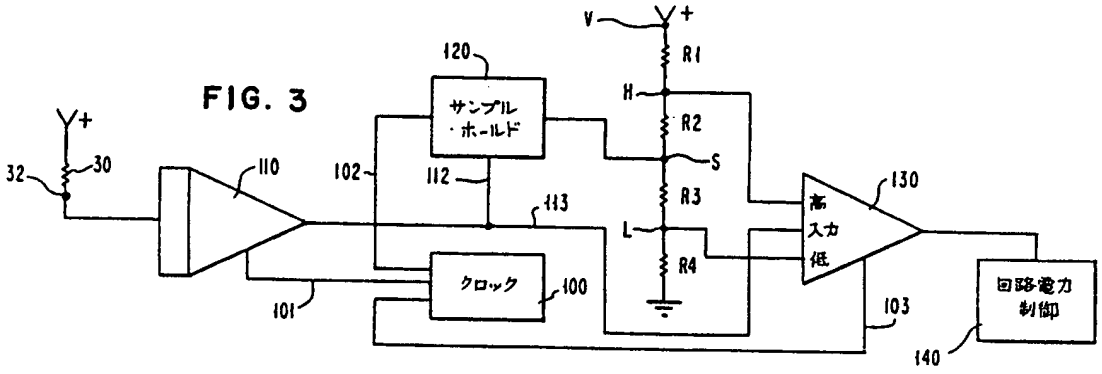


FIG. 4

FIG. 3


V
+
R1
120
サンプル
・ホールド
H
R2
S
R3
L
R4
32
30
110
102
112
113
高
入力
低
130
クロック
100
101
103
回路電力
制御
140